Is All Risk Accounted For?

Anurag Shankar
Center for Applied Cybersecurity Research
Indiana University

AMC Conference on Privacy and Security 2019

Outline

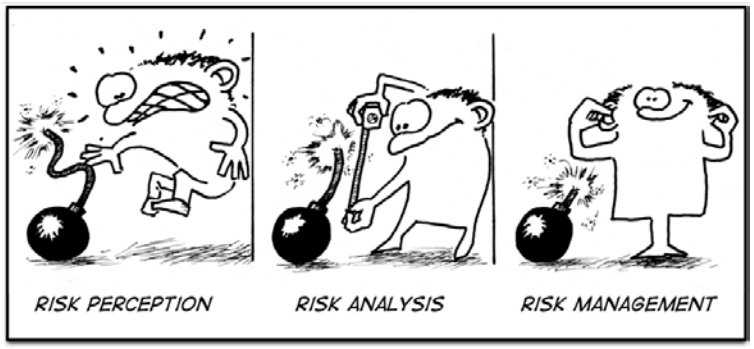
- Background
- Risk revisited
- Risk management 2.0

Background

- Researcher (11 yrs).
- Central IT provider (12 years).
- Security & compliance (12 years).

Risk revisited

1. Controls
2. Risk assessments
3. Attitude

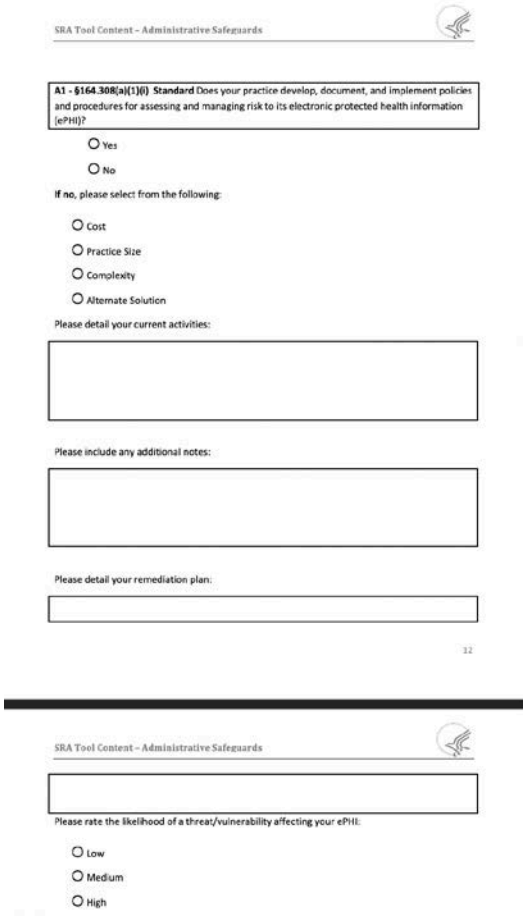


Risk #1. Controls

What does “NIST” bring to mind?

- NIST 800-53/171 - control catalogs!
- Key docs are 800-37, 30, 39.

Risk #2. Risk assessments are …



SRA Tool Content – Administrative Safeguards

A1 - §164.308(a)(1)(i) Standard Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its electronic protected health information (ePHI)?

- O Yes
- O No

If no, please select from the following:

- O Cost
- O Practice Size
- O Complexity
- O Alternate Solution

Please detail your current activities:

Please include any additional notes:

Please detail your remediation plan:

12

SRA Tool Content – Administrative Safeguards

Please rate the likelihood of a threat/vulnerability affecting your ePHI:

- O Low
- O Medium
- O High

ONC Security Risk Assessment Tool (SRA)

Arbitrary – risk depends on whose spreadsheet you use.

Risk #2. Risk assessments are …

- Static – risk remains constant once calculated.

Reality

Risk equation involves:

- Statics – risk from (risk) sources at rest, including interstitial risk.
- Dynamics – risk from sources in motion, both in space and time.

Statics

Fixed risk from (risk) sources:

- System, Endpoints
- Network
- Governance
- User
- Training
- … and how they mesh.

Dynamics

Risk evolution in space and time:

- Data movements
- Changes in time:
  - Sources
  - Threats
  - ...

Interstitial Risk

Risk from gaps between sources.

- Risk owners managing just their portion of risk.

Changing Trends

- Move to the cloud.
  - Infrastructure risk moving to cloud vendors.
  - Traditional RMFs won't apply.

C, I, A only?

- No!
- Need to add a new triad - Efficiency, Trustworthiness, Reproducibility.

Risk #3. Attitude

"The user is the weak link in the chain"

Risk #3. Attitude

~~"The user is the weak link in the chain"~~

We're driving the researchers to

WE ARE!

Where does that leave us?

Risk Management 2.0

Must:

- Treat risk properly.
- Give users what they need to succeed.

How?

- Understand what users need/do.
- Have IT/security/compliance give them risk optimized solutions.

Workflow Risk Management

- Document use cases.
- Identify ideal workflow for user.
- Assess risk from insecure workflows.
- Create secure solutions that enable the ideal workflow.

Example

Use Case	Risk Optimized Workflow
1. PI needs to do compute-intensive statistical analysis of ePHI currently on the PI's desktop. 2. Archive the results (also ePHI). 3. Make the archive accessible to research group members.	• Secure desktops/supercomputer/archiver (Dept. IT) • Install encryption software on desktops (Dept IT) • Encrypt ePHI on desktop if stored > 1 day (Dept IT/User) • Install VDI client on the desktop (Dept IT) • Launch the virtual desktop and navigate around (User) • Transfer encrypted ePHI to the supercomputer (User) • Decrypt the data on the supercomputer (User) • Use SPSS GUI within virtual desktop to do the analysis (User) • Encrypt the results (User) • Move encrypted results to the data archive /archive (User) • Set archive permissions to allow member access (Central IT) • Access the archive using institutional creds/MFA (User) • Transfer archived, encrypted ePHI to desktop (User) • Decrypt on desktop and process as necessary (User) • Encrypt archived ePHI on desktop if stored > 1 day (Dept IT/User) • Delete ePHI on desktop/supercomputer when done (User) • Securely terminate login sessions. • Document your process.

Questions?

Anurag Shankar
ashankar@iu.edu